PN-ID	B-ID	C-ID	MAC	CHKSUM
1	4 or 6	4	4 or 6	1

FIG. 1
(PRIOR ART)

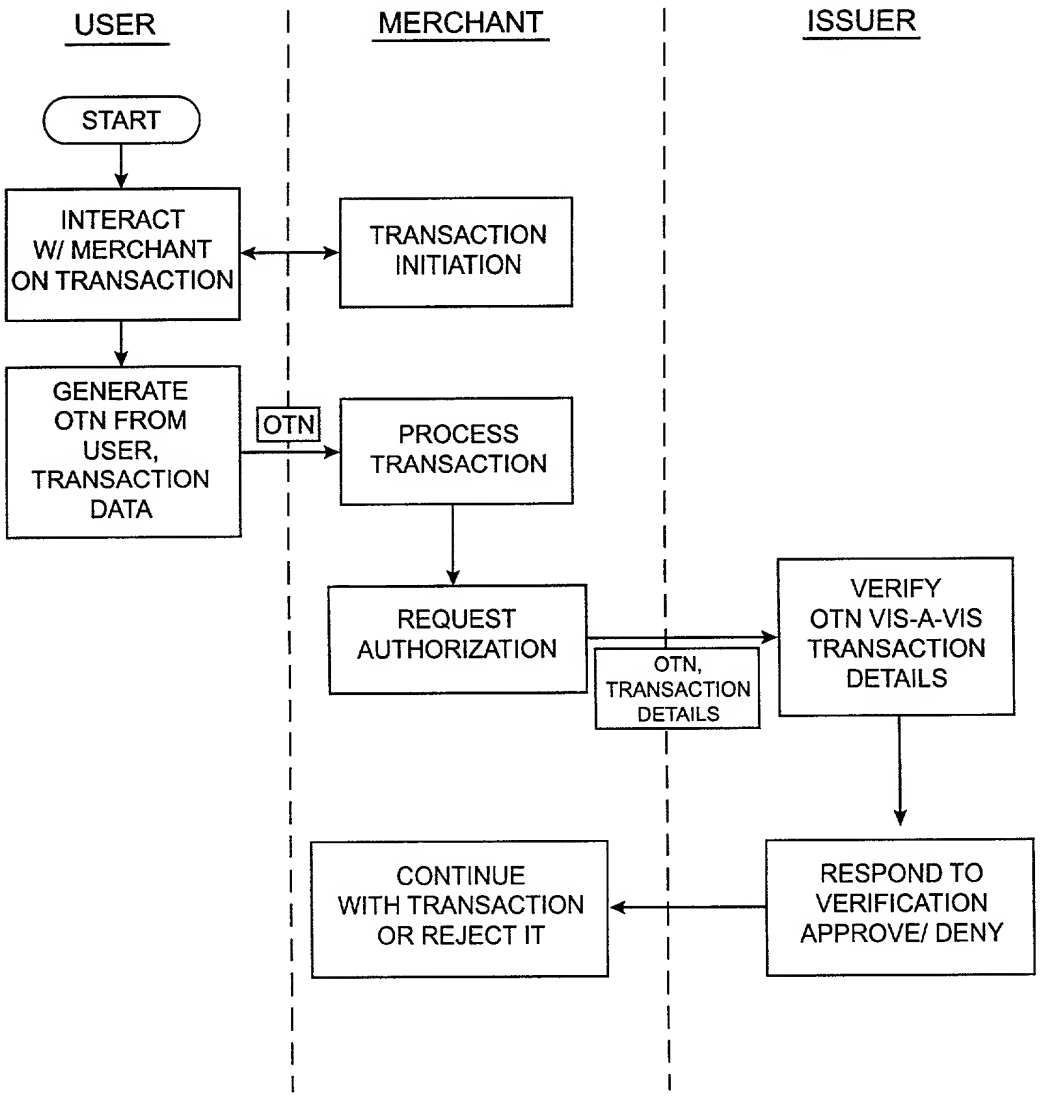

FIG. 2
(PRIOR ART)

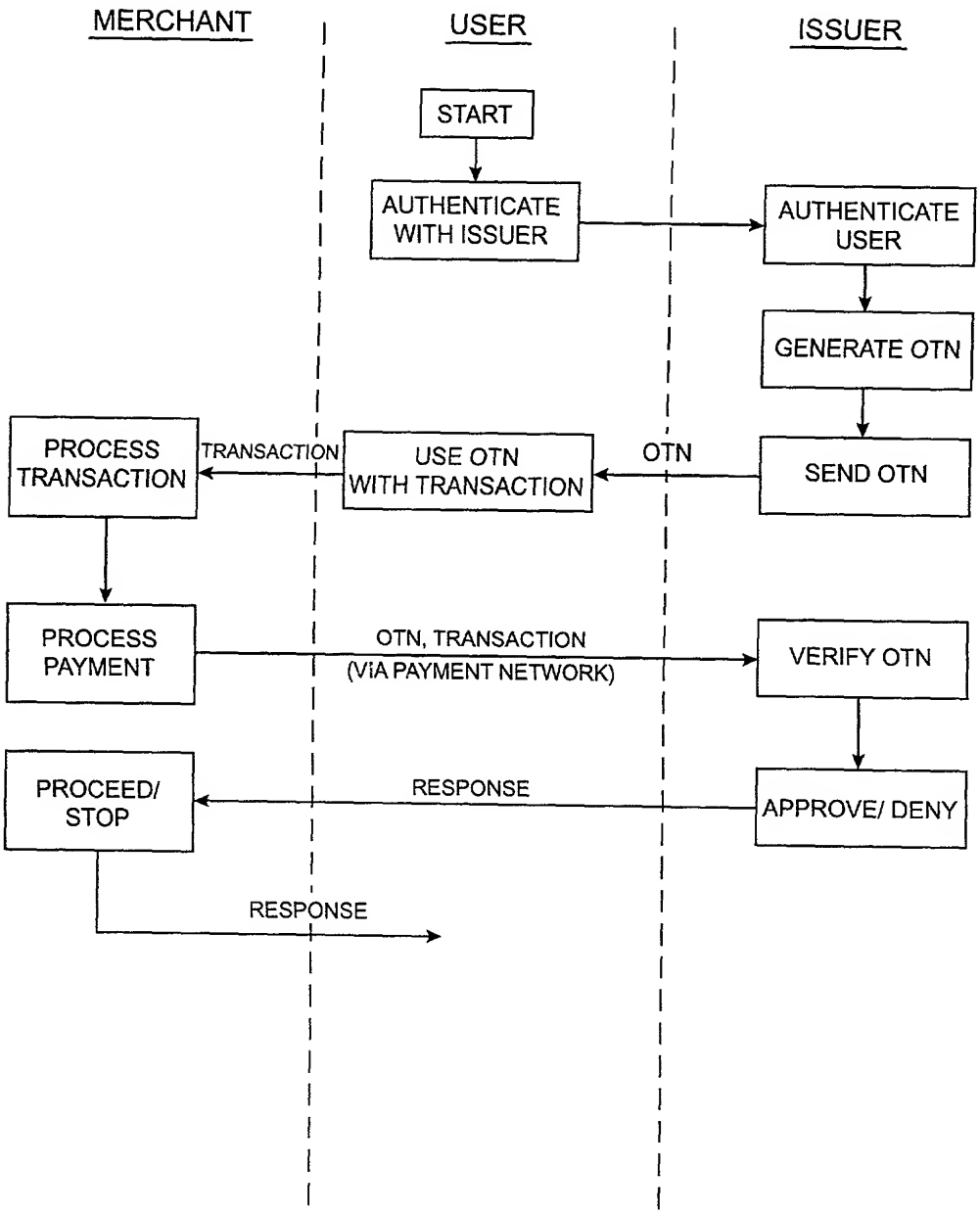

FIG. 3
(PRIOR ART)

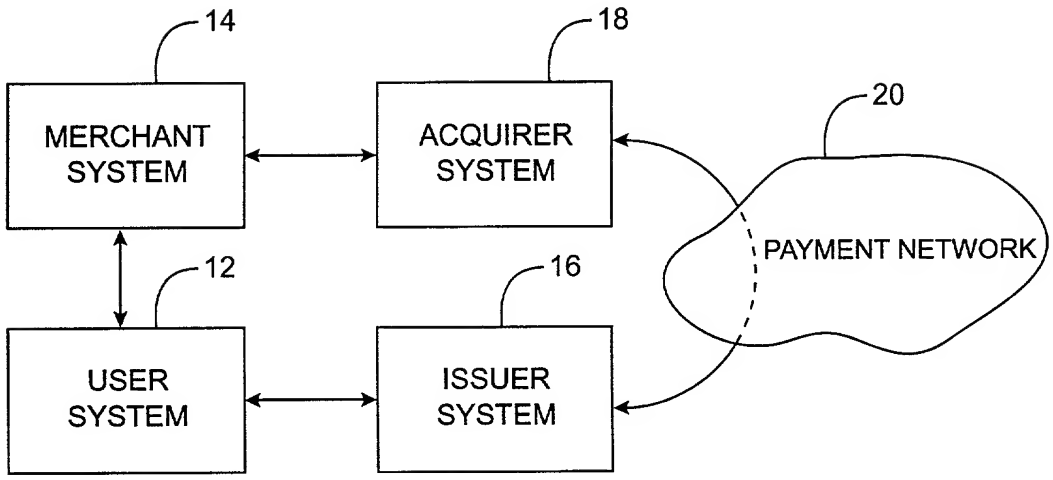
14
18
20
MERCHANT SYSTEM
ACQUIRER SYSTEM
PAYMENT NETWORK
12
16
USER SYSTEM
ISSUER SYSTEM

FIG. 4

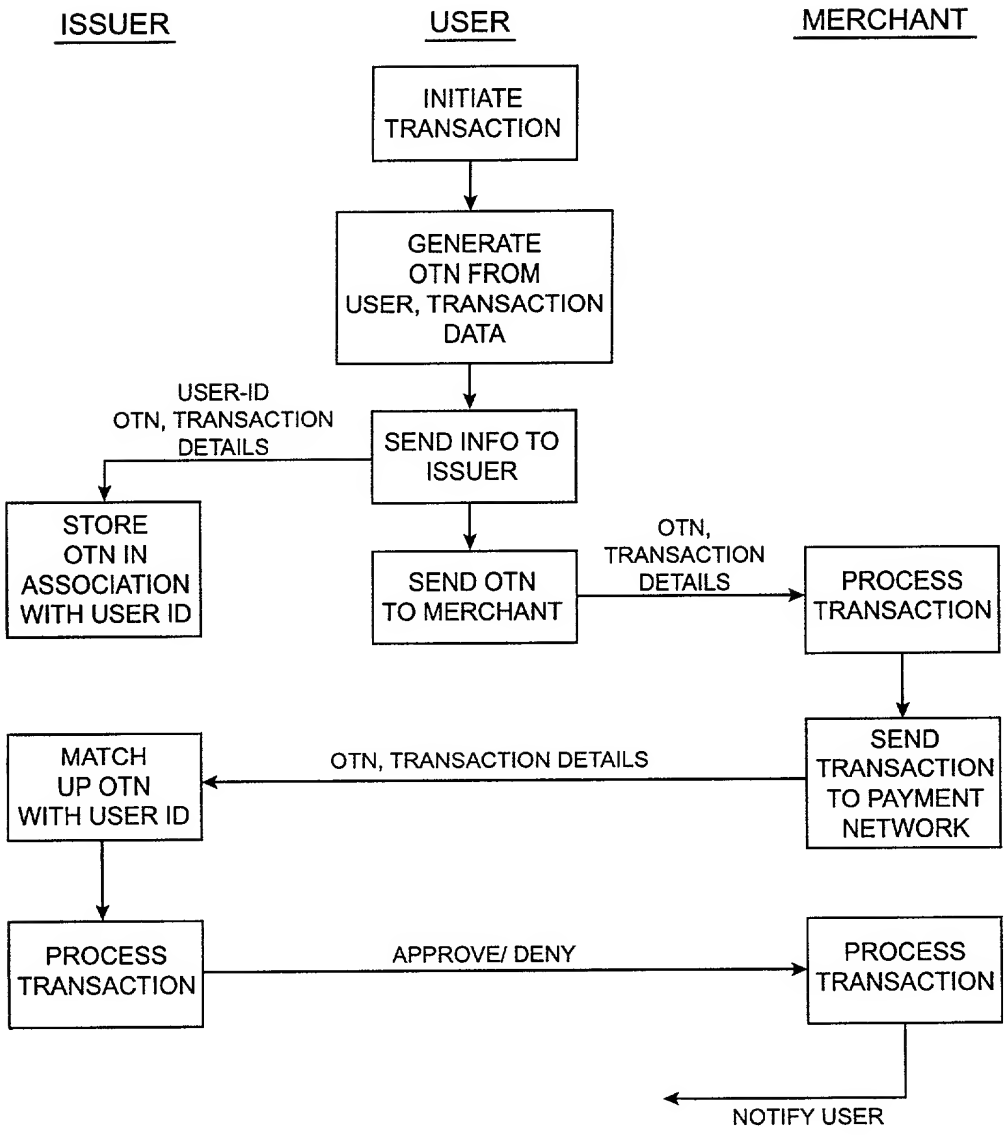
ISSUER
USER
MERCHANT
INITIATE TRANSACTION
GENERATE OTN FROM USER, TRANSACTION DATA
USER-ID
OTN, TRANSACTION DETAILS
SEND INFO TO ISSUER
STORE OTN IN ASSOCIATION WITH USER ID
SEND OTN TO MERCHANT
OTN, TRANSACTION DETAILS
PROCESS TRANSACTION
SEND TRANSACTION TO PAYMENT NETWORK
OTN, TRANSACTION DETAILS
MATCH UP OTN WITH USER ID
PROCESS TRANSACTION
APPROVE/ DENY
PROCESS TRANSACTION
NOTIFY USER

FIG. 5

6 / 8

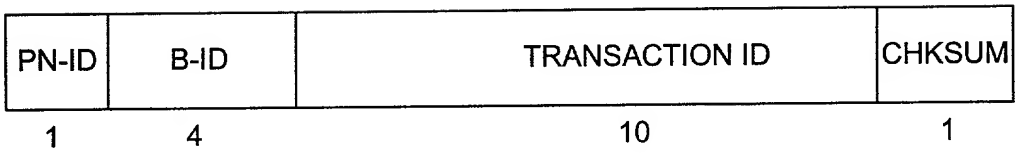

FIG. 6

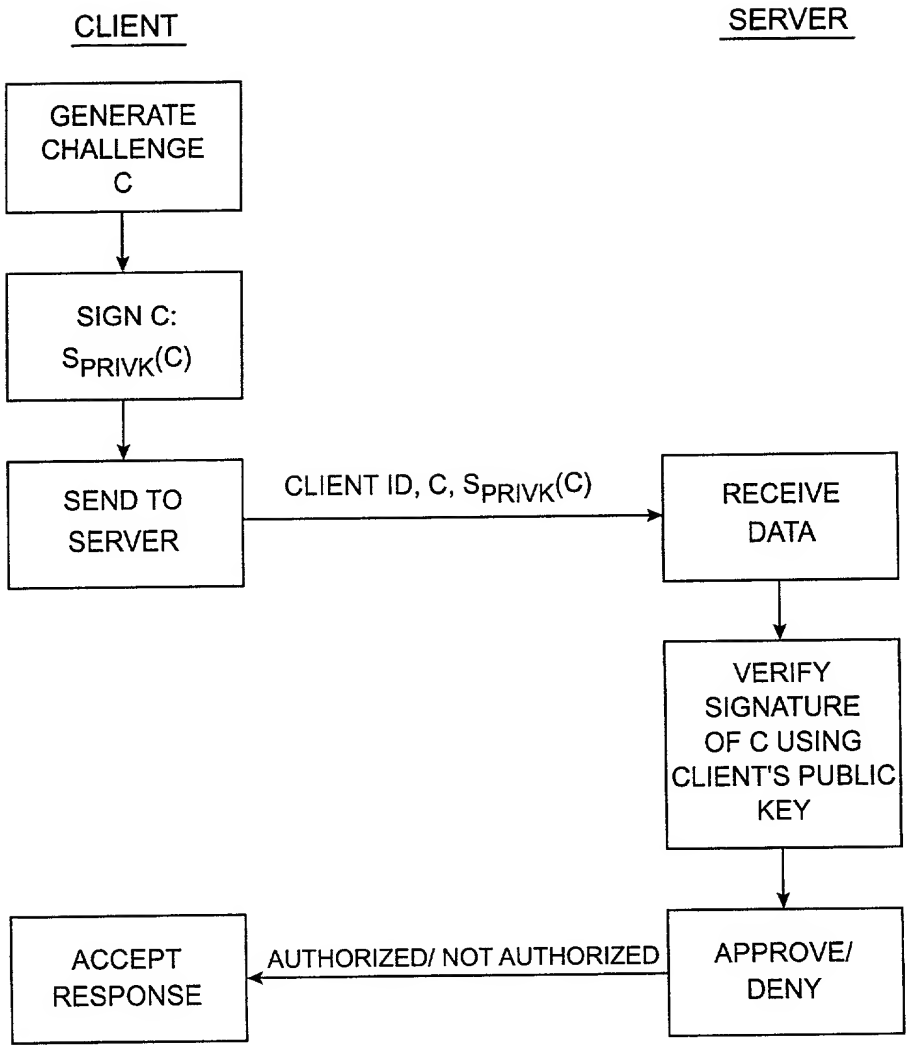
CLIENT
SERVER
GENERATE CHALLENGE C
SIGN C: $S_{PRIVK}(C)$
SEND TO SERVER
CLIENT ID, C, $S_{PRIVK}(C)$
RECEIVE DATA
VERIFY SIGNATURE OF C USING CLIENT'S PUBLIC KEY
APPROVE/ DENY
AUTHORIZED/ NOT AUTHORIZED
ACCEPT RESPONSE

FIG. 7

8 / 8

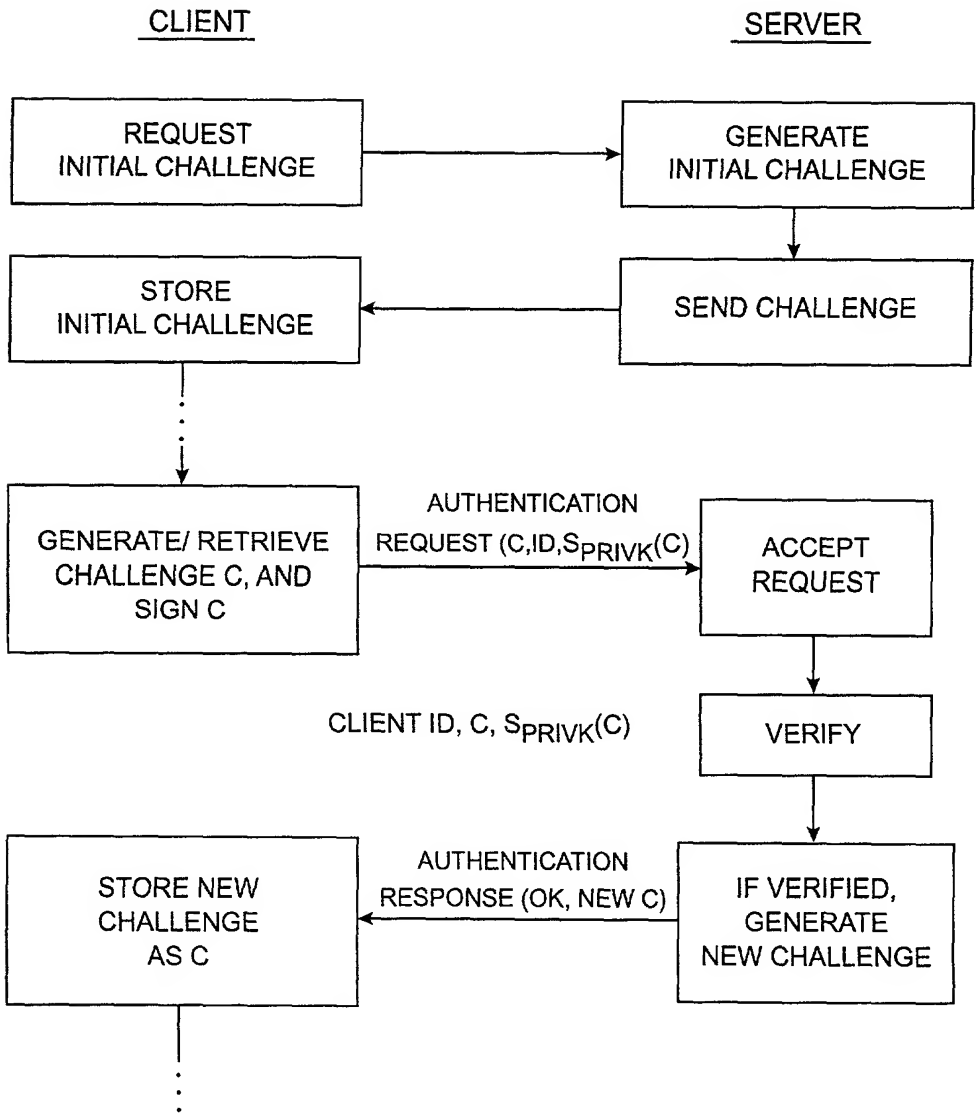
CLIENT
SERVER
REQUEST INITIAL CHALLENGE
GENERATE INITIAL CHALLENGE
STORE INITIAL CHALLENGE
SEND CHALLENGE
GENERATE/ RETRIEVE CHALLENGE C, AND SIGN C
AUTHENTICATION REQUEST (C,ID,$S_{PRIVK}(C)$)
ACCEPT REQUEST
CLIENT ID, C, $S_{PRIVK}(C)$
VERIFY
STORE NEW CHALLENGE AS C
AUTHENTICATION RESPONSE (OK, NEW C)
IF VERIFIED, GENERATE NEW CHALLENGE

FIG. 8